



DEPARTMENT OF VETERANS AFFAIRS

PRIVACY ACT OF 1974; SYSTEM OF RECORDS

AGENCY: Department of Veterans Affairs (VA), Veterans Health Administration (VHA).

ACTION: Notice of a Modified System of Records.

SUMMARY: As required by the Privacy Act of 1974, notice is hereby given that the Department of Veterans Affairs (VA) is modifying the system of records entitled "VHA Corporate Data Warehouses-VA" (172VA10A7) as set forth in the Federal Register. VA is modifying the system of records by revising the System Number; System Manager; Purposes of the System; Categories of Records in the System; Record Source Categories; Policies and Practices for Storage of Records; Physical, Procedural and Administrative Safeguards; Record Access Procedure; Notification Procedure; and Appendix. VA is republishing the system notice in its entirety.

DATES: Comments on this modified system of records must be received no later than 30 days after date of publication in the Federal Register. If no public comment is received during the period allowed for comment or unless otherwise published in the Federal Register by VA, the modified system of records will become effective a minimum of 30 days after date of publication in the Federal Register. If VA receives public comments, VA shall review the comments to determine whether any changes to the notice are necessary.

ADDRESSES: Comments may be submitted through www.Regulations.gov or mailed to VA Privacy Service, 810 Vermont Avenue, NW, (005R1A), Washington, DC 20420. Comments should indicate that they are submitted in response to "VHA Corporate Data

Warehouses-VA” (172VA10A7). Comments received will be available at [regulations.gov](https://www.regulations.gov) for public viewing, inspection or copies.

FOR FURTHER INFORMATION CONTACT: Stephania Griffin, VHA Privacy Officer, Department of Veterans Affairs, 810 Vermont Avenue, NW, Washington, DC 20420; telephone number (704) 245-2492 (Note: not a toll-free number); Stephania.Griffin@va.gov.

SUPPLEMENTARY INFORMATION: The System Number is being updated from 172VA10A7 to 172VA10 to reflect the current VHA organizational routing symbol.

The System Manager is being modified to change Assistant Deputy Under Secretary for Health Informatics to the Chief Health Informatics Officer.

Record Access Procedure and Notification Procedure are being modified to change 10A7 to 105HIG.

The Purpose of the System is being modified to include, the system may perform calculations and derive data using machine learning, natural language processing, and other artificial intelligence tools to create additional data that is validated, stored, and then made available to system users for the other purposes described within this section.

Categories of Records in the System is being modified to change Virtual Lifetime Electronic Record (VLER)-VA (168VA10P2) to Health Information Exchange–VA (168VA005). Number 13 is being added to include personal medical device data, e.g. glucometers and step counters. Being added is Number 14, Data derived from the above via calculations, machine learning, automated natural language processing, and other artificial intelligence tools, and in addition, may include manually entered data confirming derived data results.

The Record Source Categories is being modified to add VA electronic health record system and State Agencies. In addition, an example of a Federal Agency in the

form of the Centers for Disease Control (CDC) and the following VA systems of records, namely, Patient Medical Records—VA (24VA10A7); Patient National Databases—VA (121VA10A7) and from Health Information Exchange—VA (168VA005); and Revenue Program Billing and Collection Records—VA (114VA10).

Policies and Practices for Storage of Records is being modified to include Austin Information Technology Center and the VA Enterprise Cloud.

Physical, Procedural and Administrative Safeguards is being modified to include Number 6, VA Enterprise Cloud data storage conforms to security protocols as stipulated in VA Directives 6500 and 6517. Access control standards are stipulated in specific agreements with cloud vendors to restrict and monitor access.

VA Appendix A is being modified to include VA Enterprise Cloud, Microsoft Azure Data Lake and VA Common Operating Picture, Palantir Foundry, both are located at participating servers in the United States.

The Report of Intent to Modify a System of Records Notice and an advance copy of the system notice have been sent to the appropriate Congressional committees and to the Director of the Office of Management and Budget (OMB) as required by the Privacy Act of 1974 and guidelines issued by OMB, December 12, 2000.

Signing Authority

The Senior Agency Official for Privacy, or designee, approved this document and authorized the undersigned to sign and submit the document to the Office of the Federal Register for publication electronically as an official document of the Department of Veterans Affairs. Neil C. Evans, M.D., Chief Officer, Connected Care, Performing the Delegable Duties of the Assistant Secretary for Information and Technology and Chief Information Officer, approved this document on November 15, 2021 for publication.

Dated: December 17, 2021.

Amy L. Rose,

Program Analyst,

VA Privacy Service,

Office of Information Security,

Office of Information and Technology,

Department of Veterans Affairs.

SYSTEM NAME AND NUMBER: “VHA Corporate Data Warehouses-VA” (172VA10)

SECURITY CLASSIFICATION: Unclassified.

SYSTEM LOCATION: Records are located in VA National Data Centers and contracted data centers listed in Appendix A.

SYSTEM MANAGER(S): Officials responsible for policies and procedures: Charles Hume, Chief Health Informatics Officer (105), Department of Veterans Affairs, 810 Vermont Avenue, NW, Washington, DC 20420. Telephone number (202) 461-5834 (Note: not a toll-free number); Charles.Hume@va.gov.

Officials maintaining this system of records: John Quinn, Director, National Data Systems (105HIG), Austin Information Technology Center, 1615 Woodward Street, Austin, TX 78772. Telephone number (512) 326-6188 (Note: not a toll-free number); John.Quinn@va.gov.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM: Title 38, United States Code, Section 501.

PURPOSE(S) OF THE SYSTEM: The records and information may be used for clinical decision support, mobile applications presenting patient data, statistical analysis to produce various management, workload tracking, and follow-up reports; to track and evaluate the ordering and delivery of equipment, services and patient care; for the planning, distribution and utilization of resources; to monitor the performance of Veterans Integrated Service Networks (VISNs); and to allocate clinical and administrative support to patient medical care. The data may be used for VA's extensive research programs in accordance with VA policy and to monitor for bio-terrorist activity. In addition, the data may be used to assist in workload allocation for patient treatment services including provider panel management, nursing care, clinic appointments, surgery, diagnostic and therapeutic procedures; to plan and schedule training activities for employees; for audits, reviews and investigations conducted by the

Network Directors Office and VA Central Office; for quality assurance audits, reviews and investigations; for law enforcement investigations; for reporting purposes for Veterans Authorizations and Preferences and other Veterans Health Information Exchange (VHIE) reporting needs; and for health care operations and for personnel management, evaluation and employee ratings, and performance evaluations. The system may perform calculations and derive data using machine learning, natural language processing, and other artificial intelligence tools to create additional data that is validated, stored, and then made available to system users for the other purposes described within this section.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM: The records contain information for all individuals:

- (1) receiving health care from VHA;
- (2) receiving health care from Department of Defense (DoD);
- (3) providing the health care;
- (4) or working for VA or DoD.

Individuals encompass Veterans, members of the armed services, current and former employees, trainees, caregivers, contractors, sub-contractors, consultants, volunteers, and other individuals working collaboratively with VA.

CATEGORIES OF RECORDS IN THE SYSTEM: The records may include information related to:

1. Patient health record detailed information, including information from Patient Medical Records—VA (24VA10A7) and Patient National Databases—VA (121VA10A7) and from Health Information Exchange—VA (168VA005).
2. The record may include identifying information (e.g., name, birth date, death date, admission date, discharge date, gender, Social Security number, taxpayer identification number); address information (e.g., home and/or mailing address, home telephone

number, emergency contact information such as name, address, telephone number, and relationship); prosthetic and sensory aid serial numbers; health record numbers; integration control numbers; information related to medical examination or treatment (e.g., location of VA medical facility providing examination or treatment, treatment dates, medical conditions treated or noted on examination); information related to military service and status;

3. Patient health insurance information, including information from Revenue Program Billing and Collection Records—VA (114VA10);

4. Medical benefit and eligibility information, including information from Revenue Program Billing and Collection Records—VA (114VA10);

5. Patient aggregate workload data such as admissions, discharges, and outpatient visits; resource utilization such as laboratory tests, x-rays, pharmaceuticals, prosthetics and sensory aids; employee workload and productivity data;

6. Information on services or products needed in the provision of medical care (i.e., pacemakers, prosthetics, dental implants, hearing aids, etc.); data collected may include vendor name and address, details about and/or evaluation of service or product, price/fee, dates purchased and delivered;

7. Health care practitioners' name, identification number and other demographic information related to position;

8. Employees salary and benefit information;

9. Financial Information from the Financial Management System;

10. Human resource information including employee grade, salary, and tour of duty;

11. Compensation and pension determinations, Veteran eligibility, and other information associated administering Veteran benefits by the Veterans Benefit Administration;

12. Data from other Federal agencies;

13. Patient self-entered data (online forms, personal medical device data, e.g., data from glucometers and step counters)

14. Data derived from the above via calculations, machine learning, automated natural language processing, and other artificial intelligence tools, and in addition, may include manually entered data confirming derived data results.

RECORD SOURCE CATEGORIES: Information in this system of records is provided by Veterans, VA employees, VA computer systems, Veterans Health Information Systems and Technology Architecture (VistA), VA electronic health record system, contracted computer systems, VA Medical Centers, VA Program Offices, VISNs, DoD, other Federal Agencies, such as the Centers for Disease Control (CDC), State Agencies, and non-VA health care providers, and the following VA systems of records, namely, Patient Medical Records—VA (24VA10A7); Patient National Databases—VA (121VA10A7) and from Health Information Exchange—VA (168VA005); and Revenue Program Billing and Collection Records—VA (114VA10).

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING

CATEGORIES OF USERS AND THE PURPOSES OF SUCH USES: To the extent that records contained in the system include information protected by 45 CFR Parts 160 and 164, *i.e.*, individually identifiable health information, and 38 U.S.C. 7332, *i.e.*, medical treatment information related to drug abuse, alcoholism or alcohol abuse, sickle cell anemia or infection with the human immunodeficiency virus, that information cannot be disclosed under a routine use unless there is also specific statutory authority in 38 U.S.C. 7332 and regulatory authority in 45 CFR Parts 160 and 164 permitting disclosure.

1. VA may disclose information that, either alone or in conjunction with other information, indicates a violation or potential violation of law, whether civil, criminal, or

regulatory in nature, to a Federal, state, local, territorial, tribal, or foreign law enforcement authority or other appropriate entity charged with the responsibility of investigating or prosecuting such violation or charged with enforcing or implementing such law. The disclosure of the names and addresses of Veterans and their dependents from VA records under this routine use must also comply with the provisions of 38 U.S.C. 5701.

2. Disclosure may be made to any source from which additional information is requested (to the extent necessary to identify the individual, inform the source of the purpose(s) of the request, and to identify the type of information requested), when necessary to obtain information relevant to an individual's eligibility, care history, or other benefits.

3. VA may disclose information to a Federal agency, except the United States Postal Service, or to the District of Columbia government, in response to its request, in connection with that agency's decision on the hiring, transfer, or retention of an employee, the issuance of a security clearance, the letting of a contract, or the issuance of a license, grant, or other benefit by that agency.

4. VA may disclose information to a Member of Congress or staff acting upon the Member's behalf when the Member or staff requests the information on behalf of, and at the request of, the individual who is the subject of the record.

5. VA may disclose information to National Archives and Records Administration (NARA) in records management inspections conducted under 44 U.S.C. 2904 and 2906, or other functions authorized by laws and policies governing NARA operations and VA records management responsibilities.

6. VA may disclose information to the Department of Justice (DoJ), or in a proceeding before a court, adjudicative body, or other administrative body before which VA is authorized to appear, when:

- (a) VA or any component thereof;
- (b) Any VA employee in his or her official capacity;
- (c) Any VA employee in his or her individual capacity where DoJ has agreed to represent the employee; or
- (d) The United States, where VA determines that litigation is likely to affect the agency or any of its components,

is a party to such proceedings or has an interest in such proceedings, and VA determines that use of such records is relevant and necessary to the proceedings.

7. VA may disclose information to a Federal agency, a state or local government licensing board, the Federation of State Medical Boards, or a similar non-governmental entity that maintains records concerning individuals' employment histories or concerning the issuance, retention, or revocation of licenses, certifications, or registration necessary to practice an occupation, profession, or specialty, to inform such non-governmental entities about the health care practices of a terminated, resigned, or retired health care employee whose professional health care activity so significantly failed to conform to generally accepted standards of professional medical practice as to raise reasonable concern for the health and safety of patients in the private sector or from another Federal Agency. These records may also be disclosed as part of an ongoing computer matching program to accomplish these purposes.

8. VA may disclose to a Federal agency, licensing boards or the appropriate non-government entities about the health care practices of a terminated, resigned or retired health care employee whose professional health care activity so significantly failed to conform to generally accepted standards of professional medical practice, as to raise reasonable concern for the health and safety of patients receiving medical care in the private sector or from another Federal agency.

9. VA may disclose information to survey teams of the Joint Commission, College of American Pathologists, American Association of Blood Banks, and similar national accreditation agencies or boards with which VA has a contract or agreement to conduct such reviews, as relevant and necessary for the purpose of program review or the seeking of accreditation or certification.

10. VA may disclose to a national certifying body which has the authority to make decisions concerning the issuance, retention or revocation of licenses, certifications or registrations required to practice a health care profession, when requested in writing by an investigator or supervisory official of the national certifying body for the purpose of making a decision concerning the issuance, retention or revocation of the license, certification or registration of a named health care professional.

11. VA may disclose information identified in 5 U.S.C. 7114(b)(4) to officials of labor organizations recognized under 5 U.S.C. Chapter 71 when relevant and necessary to their duties of exclusive representation concerning personnel policies, practices, and matters affecting working conditions.

12. VA may disclose to the VA-appointed representative of an employee of all notices, determinations, decisions, or other written communications issued to the employee in connection with an examination ordered by VA under medical evaluation (formerly fitness-for-duty) examination procedures or Department filed disability retirement procedures.

13. VA may disclose information to the Merit Systems Protection Board (MSPB) and the Office of the Special Counsel in connection with appeals, special studies of the civil service and other merit systems, review of rules and regulations, investigation of alleged or possible prohibited personnel practices, and such other functions promulgated in 5 U.S.C. 1205 and 1206, or as authorized by law.

14. VA may disclose information to the Equal Employment Opportunity Commission (EEOC) in connection with investigations of alleged or possible discriminatory practices, examination of Federal affirmative employment programs, or other functions of the Commission as authorized by law.

15. VA may disclose information to the Federal Labor Relations Authority (FLRA) in connection with: the investigation and resolution of allegations of unfair labor practices, the resolution of exceptions to arbitration awards when a question of material fact is raised; matters before the Federal Service Impasses Panel; and the investigation of representation petitions and the conduct or supervision of representation elections.

16. VA may disclose information from this system to epidemiological and other research facilities approved by the Under Secretary for Health for research purposes determined to be necessary and proper, provided that the names and addresses of Veterans and their dependents will not be disclosed unless those names and addresses are first provided to VA by the facilities making the request.

17. VA may disclose the names and address(es) of present or former members of the armed services or their beneficiaries: (1) to a nonprofit organization if the release is directly connected with the conduct of programs and the utilization of benefits under Title 38, and (2) to any criminal or civil law enforcement governmental agency or instrumentality charged under applicable law with the protection of the public health or safety, if a qualified representative of such organization, agency, or instrumentality has made a written request that such names or addresses be provided for a purpose authorized by law; provided that the records will not be used for any purpose other than that stated in the request and that organization, agency, or instrumentality is aware of the penalty provision of 38 U.S.C. 5701(f).

18. VA may disclose information to contractors, grantees, experts, consultants, students, and others performing or working on a contract, service, grant, cooperative

agreement, or other assignment for VA, when reasonably necessary to accomplish an agency function related to the records.

19. VA may disclose to other Federal agencies to assist such agencies in preventing and detecting possible fraud or abuse by individuals in their operations and programs.

20. VA may disclose any information or records to appropriate agencies, entities, and persons when (1) VA suspects or has confirmed that there has been a breach of the system of records; (2) VA has determined that as a result of the suspected or confirmed breach there is a risk to individuals, VA (including its information systems, programs, and operations), the Federal Government, or national security; and (3) the disclosure made to such agencies, entities, or persons is reasonably necessary to assist in connection with VA efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm.

21. VA may disclose information from this system to a Federal agency for the purpose of conducting research and data analysis to perform a statutory purpose of that Federal agency upon the prior written request of that agency, provided that there is legal authority under all applicable confidentiality statutes and regulations to provide the data and VA has determined prior to the disclosure that VA data handling requirements are satisfied.

22. VA may disclose information from this system of records to OMB for the performance of its statutory responsibilities for evaluating Federal programs.

23. VA may disclose this information to the DoD for joint ventures between the two Departments to promote improved patient care, better health care resource utilization, and formal research studies.

24. VA may disclose information from this system to another Federal agency or Federal entity, when VA determines that information from this system of records is reasonably necessary to assist the recipient agency or entity in (1) responding to a suspected or

confirmed breach or (2) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs, and operations), the Federal Government, or national security, resulting from a suspected or confirmed breach.

25. VA may disclose relevant information to health plans, quality review and/or peer review organizations in connection with the audit of claims or other review activities to determine quality of care or compliance with professionally accepted claims processing standards.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS: Records are maintained on Storage Area Networks, both in Austin Information Technology Center and the VA Enterprise Cloud.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS: Records are retrieved by name, Social Security number or other assigned identifiers of the individuals on whom they are maintained.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS: Records are maintained and disposed of in accordance with General Records Schedule 20, item 4, which provides for deletion of data files when the agency determines that the files are no longer needed for administrative, legal, audit, or other operational purposes.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:

1. Access to and use of VA data warehouses are limited to those persons whose official duties require such access, and the VA has established security procedures to ensure that access is appropriately limited. Information security officers and system data stewards review and authorize data access requests. VA regulates data warehouse access with security software that relies on network authentication. VA requires information security training to all staff and instructs staff on the responsibility each person has for safeguarding data confidentiality.

2. Physical access to computer rooms housing VA data warehouses are restricted to authorized staff and protected by a variety of security devices. Unauthorized employees, contractors, and other staff are not allowed in computer rooms.
3. Data transmissions between VA operational systems and VA data warehouses maintained by this system of record are protected by state-of-the-art telecommunication software and hardware. This may include firewalls, intrusion detection devices, encryption, and other security measures necessary to safeguard data as it travels across the VA Wide Area Network.
4. In most cases, copies of back-up computer files are maintained at off-site locations.
5. Access to Cerner Technology Centers is generally restricted to Cerner employees, contractors or associates with a Cerner issued ID badge and other security personnel cleared for access to the data center. Access to computer rooms housing Federal data, hence Federal enclave, is restricted to persons Federally cleared for Federal enclave access through electronic badge entry devices. All other persons, such as custodians, gaining access to Federal enclave are escorted.
6. VA Enterprise Cloud data storage conforms to security protocols as stipulated in VA Directives 6500 and 6517. Access control standards are stipulated in specific agreements with cloud vendors to restrict and monitor access.

RECORD ACCESS PROCEDURE: Individuals seeking information regarding access to and contesting of records contained in this system of records may write to the Director of National Data Systems (105HIG), Austin Information Technology Center, 1615 Woodward Street, Austin, TX 78772. Inquiries should include the person's full name, Social Security number, location and dates of employment or location and dates of treatment, and their return address.

CONTESTING RECORD PROCEDURES: (See Record Access Procedures above.)

NOTIFICATION PROCEDURE: Individuals who wish to determine whether this system of records contains information about them should contact the Director of National Data Systems (105HIG), Austin Information Technology Center, 1615 Woodward Street, Austin, TX 78772. Inquiries should include the person's full name, Social Security number, location and dates of employment or location and dates of treatment, and their return address.

EXEMPTIONS PROMULGATED FOR THE SYSTEM: None.

HISTORY: Last full publication provided in 85 FR 52415 dated August 25, 2020.

VA APPENDIX A:

Database Name	Location
Corporate Data Warehouse	Austin Information Technology Center, 1615 Woodward Street, Austin, TX 78772.
HealthIntent at Cerner Technology Centers (CTC)	Primary Data Center Kansas City, MO Continuity of Operations/Disaster Recovery (COOP/DR) Data Center Lee Summit, MO
VA Common Operating Picture, Palantir Foundry	Participating servers in the United States
VA Enterprise Cloud, Microsoft Azure Data Lake	Participating servers in the United States
VA Informatics and Computing Infrastructure (VINCI)	Austin Information Technology Center 1615 Woodward Street Austin, TX 78772

